Emerging Standards
Editors: Ramaswamy Chandramouli, mouli@nist.gov
Rick Kuhn, kuhn@nist.gov
Susan Landau, susan.landau@sun.com

Who's Watching You Now?

Location-based applications and services are emerging at a pace that's likely to accelerate over the next few years. Such services offer everything from consumer convenience to life-saving security:

John Morris
Center for Democracy & Technology

Jon Peterson
NeuStar

- An out-of-town visitor wants directions to the closest Starbucks, but the visitor's network wants to serve up an advertisement for a competing coffee shop.
- An armored transport company needs to track each of its trucks in real time.
- A father gives his child a device that automatically "checks in" whenever it can connect to an open WiFi network.
- A corporate CEO wants her family to be able to find her at any time; she wants other corporate officers to have access to that information as well—except when she's in a highly confidential meeting with a competing company to discuss a merger.
- A tourist in Europe connects to a US-based voice-over-IP (VoIP) service through an Internet café, but witnesses a crime and needs to call for emergency services.

All these scenarios involve the transmission of location information over an IP network, and all raise significant issues about that information's privacy, security, and control.

The IETF's Geographic Location/Privacy working group (Geopriv WG) has created a set of standards for sending location information coupled with privacy rules over the Internet. The standards call for the creation of *location objects* (LOs), which contain a location along with a limited set of rules that can point to an external set of more complex rules, if necessary. In development over the past five years, Geopriv is approaching an initial completion stage and appears likely to be implemented in several key technologies.

Geopriv's origins

In a departure from typical IETF practice, the Geopriv WG didn't originate in a development effort—rather, the IETF's leadership initiated it in 2001. Over the years, several proposals sought to standardize the transmission of location information in an Internet Protocol (IP) environment, but those proposals largely ignored the significant privacy issues that location information raises. The IETF's Internet Engineering Steering Group concluded that privacy and security had to be an integral part of any standard to send or carry location information, which is why Geopriv's charter focuses heavily on privacy concerns (www.ietf.org/html.charters/geopriv-charter.html).

The WG's charter focused on protecting the transfer of location information over IP networks, and it specifically deemed technologies for determining location to be outside Geopriv's scope. The WG didn't attempt to define a protocol to actually transport information over the Internet—instead, the Geopriv standard calls for a "using" protocol such as HTTP or the Session Initiation Protocol (SIP) to convey location objects. Moreover, the WG didn't set out to define a new syntactical format for describing location information because quite a few were already in use in various capacities.

Geopriv basics

The Geopriv standard refers to four primary entities:[1]

- The *location generator* (LG) determines a "target's" location and then creates an LO. In some scenarios, the LG could be the target itself (such as an automobile with location-tracking components) or a proxy (such as the cell phone a target carries). The LG itself can determine its own location (with GPS technology, for example) or learn its location from another source (such as a network access provider, a Dynamic Host Configuration Protocol server, or even manual human entry of a location).
- The *location server* (LS) receives location objects from the LG and responds to requests for location information (if applicable privacy rules permit it to do so).
- The *location recipient* (LR) receives the location object from the LS (or can subscribe to a location to receive a series of locations).
- The *rule holder* (RH) stores the privacy rules to be applied to location information. One or more *rule makers* (RMs) create the rules and set the policies governing the location information's distribution.

Logically, the LS stands in the middle of the other three core elements, which, within the Geopriv framework, don't communicate with each other directly. These four roles can overlap and sometimes reside in the same physical device—in cases in which location information is pushed to a recipient, for example, the LG and LS might be composed into a single deployed entity.

Because Geopriv doesn't make assumptions about different elements' availability or capabilities, it works in a broad range of scenarios and devices, including those highly constrained in terms of bandwidth or intelligence. It also makes no assumption about where the LS is located in a network, thus permitting third-party LSs wholly unrelated to any specific network operator. Geopriv also avoids assumptions about relationships among elements and devices—for example, it doesn't assume a target is also an RM; although this might often be true, it would not be in cases such as a parent taking on the RM role to define who can track a child's cell phone.

Location object

A *location generator* (LG) can express location information in several formats, including latitude/longitude/altitude coordinates via the Geography Markup Language (GML; www.opengeospatial.org/specs/?page=specs) or more traditional street/city/region/country addresses via a scheme the Geopriv WG is currently developing.

Although Geopriv's requirements don't dictate or require any specific format for the location object, the WG did develop and promulgate a standard for a viable XML-based instantiation.[2] The PIDF-LO location object is built on top of the Presence Information Data Format (PIDF),[3] which conveys presence in XML.

One of Geopriv's requirements is that the location object "must be usable in a secure manner even by applications on constrained devices."[1] This requirement creates significant tension because a robust set of privacy rules could be too large to store or convey with constrained devices. To solve this tension, the Geopriv standard describes two sets of privacy rules—a limited set that any Geopriv location object "must" carry, and a more robust set that can be stored and referenced externally. By requiring a limited set of rules to be bound into the location object itself, Geopriv ensures that no recipient can claim ignorance of the basic privacy rules that apply to that information.

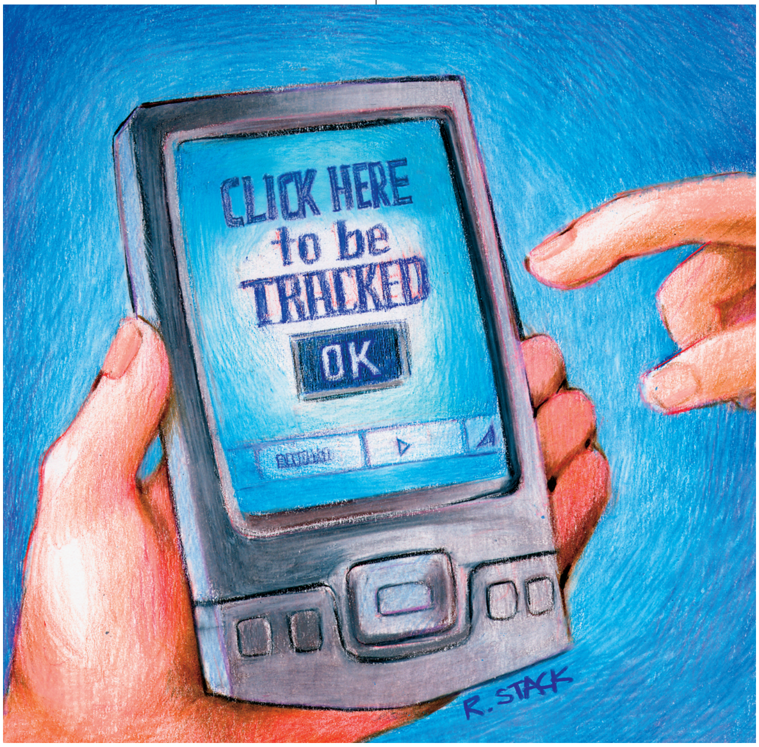
Privacy rules

The PIDF-LO standard offers a limited set of privacy rules:

- *Retention limit date and time*. The time limit isn't an indication of how long the location information remains valid, but how long it can be retained.
- *Indication of consent (or lack of consent) to retransmit location information*. For many simple location transactions (such as, "Where is the closest Starbucks to where I am right now?"), a denial of retransmission consent coupled with a very short retention time limit effectively conveys that the recipient should respond to the immediate query and then discard the location information.
- *Pointer to an external, fuller set of privacy rules for any retransmission of location information*. In the Starbucks example, no pointer is needed because no permission is granted for information retransmission (thus the LR doesn't need to know any further privacy rules).
- *Free-form text area*. This area can convey the privacy policy in human-readable form.

Although limited, these rules are sufficient to cover many forms of consumer-oriented location services, including those in which information or an immediate service is based on location (such that no continuing services are sought or expected).

The Geopriv WG has made significant progress in defining a more robust set of rules for the rule holder to store (and provide to an LS when needed).[4] The goal is to create a *common policy* framework to cover access



to location and presence information (such as "I'm online" in an instant-messaging context). At its core, this approach is based on conditions for *identity* (who can receive location information), *validity* (when an LS can provide location information), and *sphere* (the target's state, such as work, home, meeting, or travel). Ideally, these conditions should lead to rules such as, "If I'm at work, the following people can learn my location."

Identities and their conditions are deliberately additive permissions ("*x*, *y*, and *z* can receive my location") and can't be denials ("do not give my location to *a* or *b*"). Affirmative permissions can, however, have exceptions: "my location can be provided to anyone in the @example.com domain except joe@example.com." By allowing only permissions, the rules become somewhat simpler, their sequence becomes irrelevant, and—critically—their absence doesn't degrade privacy. If a rule can't be retrieved for any reason, the result will always be fewer permissions (thus more strongly preserving the information's privacy).

If a rule can't be retrieved for any reason, the result will always be fewer permissions (thus more strongly preserving the information's privacy).

Combining identity, validity, and sphere yields the conditions to answer an `IF` question: can a particular requester receive specific information at a particular time? But the common policy approach envisions transformations and actions to answer a `THEN` question: what can be provided? With transformations, an LS can reduce a location's resolution from an exact street address to just the city. Combining all these elements means fine-grained—and different—permissions for family members, bosses, coworkers, and everyone else.

One special case, however, is emergency communications. If someone dials an emergency number ("911" in the US), this action should override an RM's privacy rules and permit the transmission of location information. Although someone might want privacy rules to cover even emergency calls, many networks and service providers are legally obligated to complete such calls and transmit valid locations, so a Geopriv prohibition wouldn't likely be implemented. This requirement—that Geopriv not obstruct emergency communications—heightens the obligation to guard against spoofing and other violations. Much of the IETF's work on emergency communications for VoIP occurs in the Emergency Context Resolution with Internet Technologies (ECRIT) working group, which draws its baseline architecture from Geopriv's location-transmission standards.

Acceptance and implementation

Geopriv is only now becoming sufficiently mature for implementation, but the IETF expects that any of its standards for transmitting location information will use Geopriv to protect that information. Consequently, the Geopriv work will inform ongoing IETF work on VoIP, emergency communications, and so on.

Several standards bodies and regulatory agencies have started work with the Geopriv standards, especially in the context of emergency communications for VoIP. At the Standards Developing Organizations (SDO) Emergency Services Coordination Workshop in October 2006, an international group of more than 20 technical and governmental organizations converged to discuss the road forward for VoIP (www.ietf-ecrit.org/EmergencyWorkshop2006/). Among the bodies giving Geopriv special attention is the US National Emergency Number Association (NENA; www.nena.org), an organization implementing a staged approach to integrating VoIP into the 911 architecture. Geopriv WG members are also working on geolocation and emergency services with the Third-Generation Partnership Program (3GPP; www.3gpp.org), which specifies the Internet Multimedia Subsystem (IMS) deployment of SIP that will likely determine how VoIP will enter carrier networks in both the wireless and wireline spaces. Although it's too early to say definitively how Geopriv will affect these efforts and others around the globe, its close coupling with SIP makes it likely that we'll see it used in most SIP deployments that require location-based services.

From a privacy perspective, Geopriv offers the opportunity to convey fairly robust and potentially complex privacy rules along with location information. It can't, however, provide guarantees that those rules will be honored or followed in any given situation. Yet, Geopriv could be a critical element of a larger privacy framework (perhaps created by local law) that provides such guarantees through legal rather than technical means.

This interplay between law and technology could prove beneficial in various ways. A law could decree that no location information be distributed without the express permission of the person being tracked (aside from law enforcement or emergency cases), and Geopriv could provide the means to grant (or not grant) such permission. Alternatively, a law might allow such distribution unless the consumer takes a proactive step to deny permission; again, Geopriv could be the consumer's vehicle.

The Geopriv WG also provides a very strong example of effective collaboration between the technical standards and the public interest–public policy communities. Although neither policy advocates nor technologists have achieved everything they sought in the Geopriv process, the collaboration was very constructive. The end result should be a significant contribution to protecting privacy across IP networks. ▢

References

1. J. Cuellar et al., *Geopriv Requirements*, RFC 3693, Oct. 2003; www.ietf.org/rfc/rfc3693.txt.
2. J. Peterson, *A Presence-Based GEOPRIV Location Object Format*, RFC 4119; Dec. 2005; www.ietf.org/rfc/rfc4119.txt.
3. H. Sugano et al., *Presence Information Data Format (PIDF)*, RFC 3863, Aug. 2004; www.ietf.org/rfc/rfc3863.txt.
4. H. Schulzrinne et al., "Common Policy: A Document Format for Expressing Privacy Preferences," RFC 4745, pending approval in 2007; www.ietf.org/rfc/rfc4745.txt.

***John Morris** is an attorney with a technical background who serves as staff counsel at the Center for Democracy & Technology. He coauthored RFCs 3693 and 4745. Contact him at jmorris@cdt.org.*

***Jon Peterson** is a fellow at NeuStar. He has done extensive work on real-time communications in various standards bodies, especially the IETF, where he serves as codirector of the Real-Time Applications and Infrastructure (RAI) area. Peterson authored RFC 4119 and coauthored RFCs 3693 and 3863. Contact him at jon.peterson@neustar.biz.*